End-User Requirements for ActivCard Middleware CAC Cryptographic Logon AUGUST 2005

Submitted by

ARMY Information Assurance CAC/PKI Training

2110 Washington Boulevard, Suite 200
Arlington VA 22204

ActivCard End-User Requirements for CAC Cryptographic Logon

Introduction

The purpose of this guide is to assist Common Access Card (CAC) user's verify they have all required components necessary to facilitate the use of CAC Cryptographic Logon (CCL).

Background

A significant deterrent in the past for using the CAC to logon to network resources has been the difficulty of attaining timely DoD PKI Certificate Validation (CV) information of the CAC holder. The DoD infrastructure-supported CV solution (download of the entire DoD certificate revocation list) does not provide an adequate solution. The Army is currently working on a viable CV solution that will provide the necessary support to warrant the implementation of a CCL capability in the near future. Another major deterrent is that CCL requires a Windows 2003 network infrastructure with Active Directory (AD). The Army plans to have this infrastructure in place at most installations by summer of 2005. In addition, user workstations require smart card readers and middleware which is already widely implemented throughout the Army.

It is envisioned that a phased approach will be used to introduce the CCL capability. The initial phase was completed during a certificate validation **(CV)** operational assessment **(OA)** conducted at Fort Dix, New Jersey in January-February 2005. The CCL capability was successfully implemented during the OA and is still in use. The second phase will consist of conducting an early adopter fielding during the fall of 2005. The last phase, if approved, will allow deployment of the CCL capability Army-wide.

In order to avoid delays with future CCL implementations, we requested the Director of Information Management (DOIM), in conjunction with the Garrison Military Personnel Directorate (MPD)/ CAC issuance center; assist their local CAC user population to conform to the following user level requirements:

(1) CAC's must be configured with three Public Key Infrastructure (PKI) certificates (identity, email signature and email encryption)

(2) User's must know there 6-8 digit CAC PIN

(3) User workstations must have functioning smart card readers and middleware (ActivCard 3.0 or greater or NetSign 4.2 or greater)

(4) User workstations must have Windows 2000 or XP operating systems.

End users are responsible for verifying items 1thru 3 above.

Required Desktop Equipment

Below is a listing of the components that you will need to have in order to use CCL:

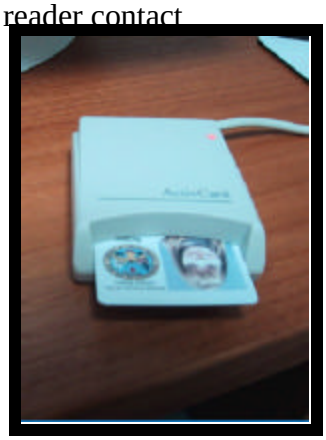
- Computer system (desktop/laptop)
- Smart card reader
- Common Access Card (CAC)

Verifying PKI Certificates

Please contact your S1, Adjutant or Civilian personnel coordinator in order for them to schedule an appointment with the local DHR ID card section for all your CAC issues.

Contact your IMO for all computer/ middleware issues.

Locate your smart card reader and verify that it is connected to your computer; this can be accomplished by following the cord leading from the card reader to the computer. If you don't have a smart card reader contact your IMO.



After logging on to your computer; locate the "System Tray ". It is located in the lower quadrant of your computer display. This is the same area that the computers clock is displayed.

Using your mouse, move your curser over top of your middleware icon and double click using the left mouse button.

ActivCard

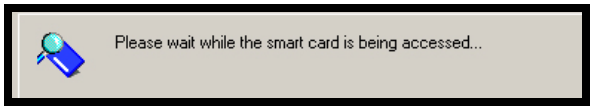
4. At this point your middleware window should open, if it doesn't; repeat again.

If there are no icons displayed then please contact your IMO.

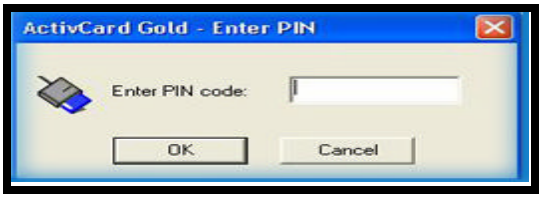
Should repeated attempts fail, please contact your IMO for middleware issues.

5. Ensure your CAC is inserted into the smart card reader so that the picture is facing up and is visible.

6. Once the card has been properly inserted into the card reader you'll get a popup window that states" please wait while the smart card is being accessed." If this window does not appear please contact your IMO.



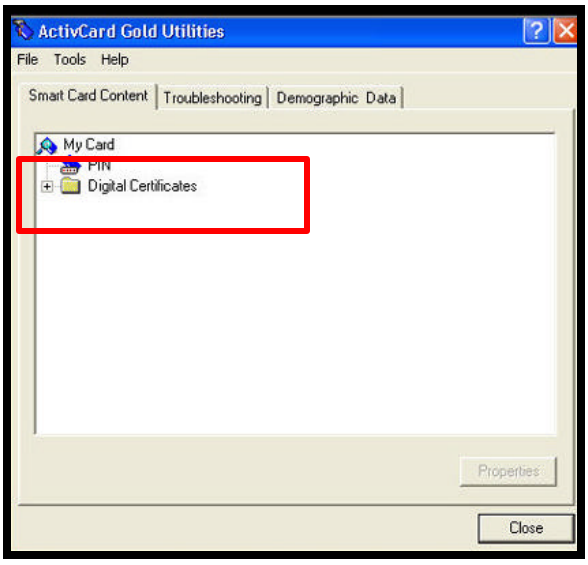
7. You may be asked to input your 6 – 8 digit CAC PIN.



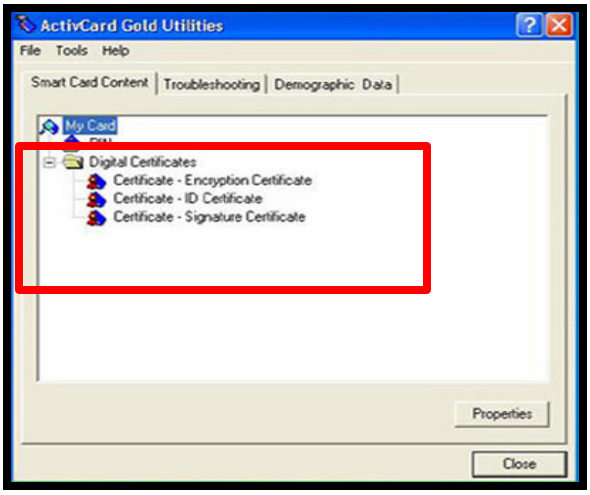
ActivCard Pin Request

If you enter your CAC PIN incorrectly three times or you have forgotten your PIN please see your S1, Adjutant or Civilian personnel coordinator or CAC PIN Reset (CPR) personnel in order to obtain a pin or have your PIN reset.

8. After the smart card reader has accessed your card you will see three tabs.
    - Smart Card Content
    - Troubleshooting
    - Demographic Data.
9. We are only going to utilize the "Smart Card Content" tab.
10. Looking at the viewing area you'll see a folder that say's" Digital Certificates".



11. Using your mouse and your left mouse button, double click on the Digital Certificates folder.



12. If you have all three PKI certificates no further action is required. Please proceed to CAC Pin Check procedures.

If you do not see all three PKI certificates take the following steps:

Missing Certificate?

No PKI Certificates

1. If you already have an Army Knowledge Online (AKO) email address (FName.LName@us.army.mil) go to DHR ID card section and have them add your PKI Identity certificate along with your two PKI email certificates (email signature and email encryption), using your AKO email address, to your CAC.
2. If you don't have an AKO email address (FName.LName@us.army.mil) go to the AKO website (https://www.us.army.mil/suite/login/welcome.html) and follow the instructions to obtain an AKO email address. Go to the DHR ID card section and have them add your PKI Identity certificate along with your two PKI email certificates (email signature and email encryption), using your AKO email address, to your CAC.
3. Have the MPD verify that you now have all three PKI certificates.
4. This concludes the ActivCard portion please proceed to the CAC Pin Check procedure.

Only have a PKI Identity certificate

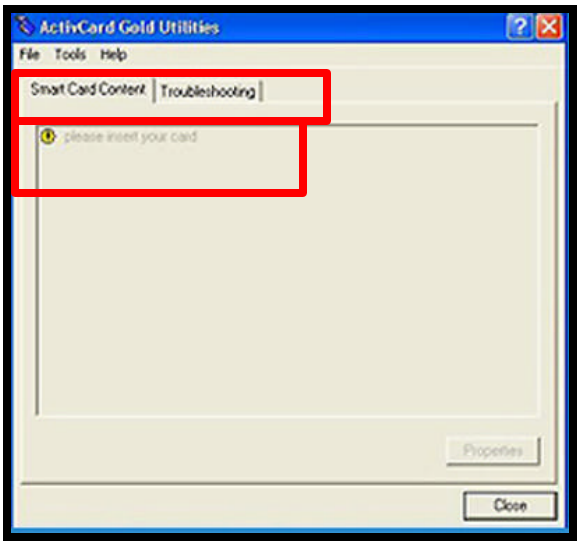
1. If you already have an Army Knowledge Online (AKO) email address (FName.LName@us.army.mil) go to the DHR ID card section and have them add your two PKI email certificates (email signature and email encryption), using your AKO email address, to your CAC.
2. If you don't have an AKO email address FName.LName@us.army.mil) go to the AKO website (https://www.us.army.mil/suite/login/welcome.html) and follow the instructions to obtain an AKO email address. Go to the DHR ID card section and have them add your two PKI email certificates (email: signature and encryption), using your AKO email address, to your CAC.
3. Ensure that you have DHR ID card section verify that you now have all three PKI certificates.
4. This concludes the ActivCard portion please proceed to the CAC Pin Check procedure.

CAC Pin Check:

In the proceeding procedures you were ask to verify your certificates, during the process you may have had to enter your "Pin". In this case you will not receive a prompt to enter your pin again as long as you have not removed your CAC from the card reader.

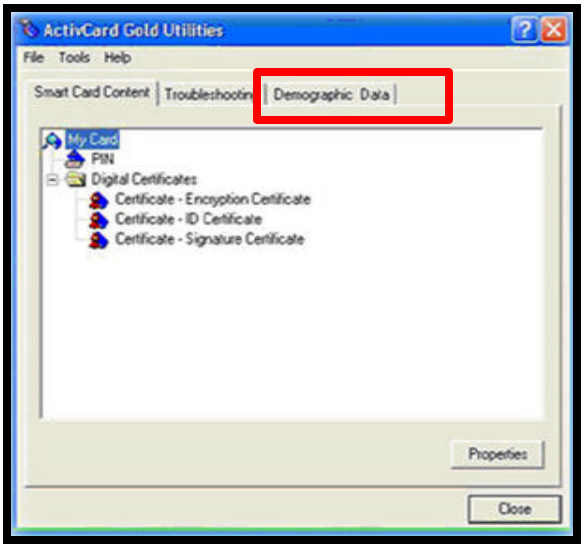
Miscellaneous Things to Keep In Mind:

1. Upon activating ActivCard you'll notice two tabs. The “Smart Card Content” and the “Troubleshooting” tab.
2. If you see a yellow exclamation point in the “Smart Card Content” information viewing area you need to insert your CAC in to the smartcard reader.



ActivCard

1. With your Middleware window open select the "Demographic" Tab from the menu bar by double clicking the left mouse button.

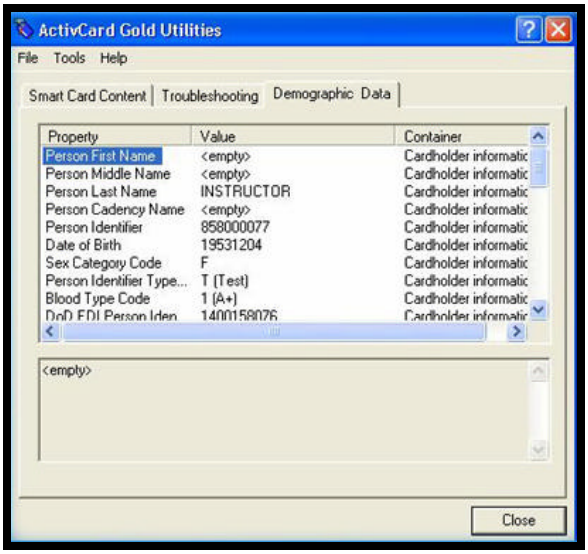


1. The "Pin Request" window will appear.

ActivCard Pin Request

2. Enter your 6-8 digit pin.

3. Once you have properly entered the pin you will be able to view all your demographic data.



4. This concludes the ActivCard CAC Pin Check.

This page Intentionally Blank